Software Supply Chain Assurance – Existing and New Standards

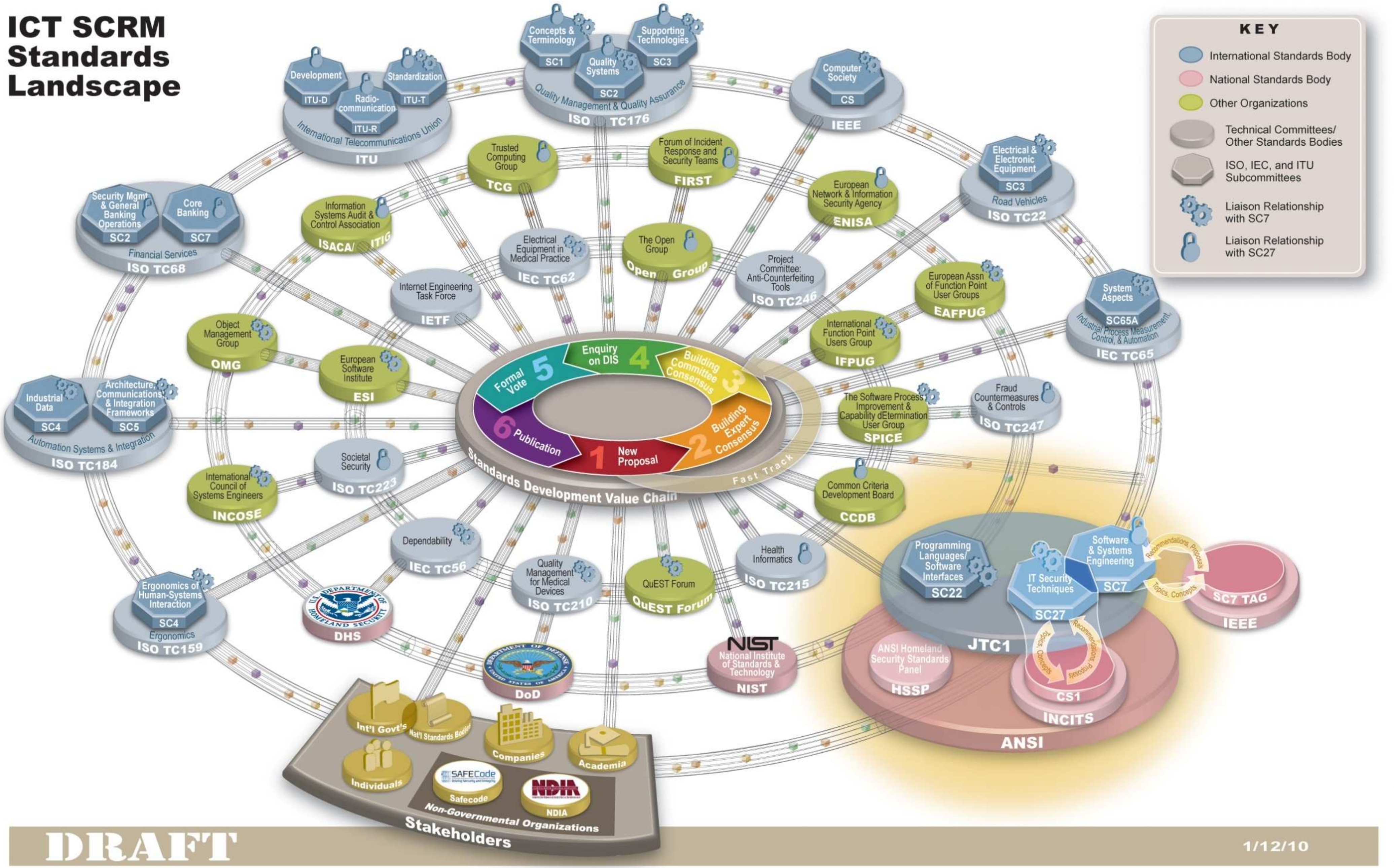
March 09, 2010

Booz | Allen | Hamilton

ICT Supply Chain Assurance Standards Landscape is Rather Complex

- ICT Supply Chain Assurance incorporates practices from
  - Information security
  - Software Assurance
  - System and software engineering
  - Supply chain and logistics
  - Other fields
- Currently there is no single standard addressing ICT Supply Chain Assurance
- However there are LOTS of standards that can be
  - Updated to integrate aspects of and pointers to ICT Supply Chain Assurance
  - Used to apply ICT Supply Chain Assurance techniques
- Furthermore, there are emerging government and industry practices that can be leveraged to enhance content of existing standards or develop specific new standard

The Landscape



ICT SCRM Standards Landscape

KEY

- International Standards Body
- National Standards Body
- Other Organizations
- Technical Committees/ Other Standards Bodies
- ISO, IEC, and ITU Subcommittees
- Liaison Relationship with SC7
- Liaison Relationship with SC27

ITU – International Telecommunications Union: ITU-D Development; ITU-T Standardization; ITU-R Radio-communication

ISO TC176 – Quality Management & Quality Assurance: SC1 Concepts & Terminology; SC2 Quality Systems; SC3 Supporting Technologies

IEEE: CS Computer Society

ISO TC22 – Road Vehicles: SC3 Electrical & Electronic Equipment

IEC TC65 – Industrial Process Measurement, Control, & Automation: SC65A System Aspects

ISO TC68 – Financial Services: SC2 Security Mgmt & General Banking Operations; SC7 Core Banking

ISO TC184 – Automation Systems & Integration: SC4 Industrial Data; SC5 Architecture, Communications, & Integration Frameworks

ISO TC159 – Ergonomics: SC4 Ergonomics of Human-Systems Interaction

TCG Trusted Computing Group

FIRST Forum of Incident Response and Security Teams

ENISA European Network & Information Security Agency

ISACA/ITIG Information Systems Audit & Control Association

IEC TC62 Electrical Equipment in Medical Practice

Open Group The Open Group

ISO TC246 Project Committee: Anti-Counterfeiting Tools

EAFPUG European Assn of Function Point User Groups

IETF Internet Engineering Task Force

OMG Object Management Group

IFPUG International Function Point Users Group

ESI European Software Institute

SPICE The Software Process Improvement & Capability dEtermination User Group

ISO TC247 Fraud Countermeasures & Controls

ISO TC223 Societal Security

INCOSE International Council of Systems Engineers

CCDB Common Criteria Development Board

IEC TC56 Dependability

ISO TC210 Quality Management for Medical Devices

QuEST Forum QuEST Forum

ISO TC215 Health Informatics

DHS

DoD

NIST National Institute of Standards & Technology

Standards Development Value Chain: 1 New Proposal; 2 Building Expert Consensus; 3 Building Committee Consensus; 4 Enquiry on DIS; 5 Formal Vote; 6 Publication; Fast Track

JTC1: SC22 Programming Languages/ Software Interfaces; SC27 IT Security Techniques; SC7 Software & Systems Engineering

IEEE: SC7 TAG

Recommendations, Proposals

Topics, Concepts

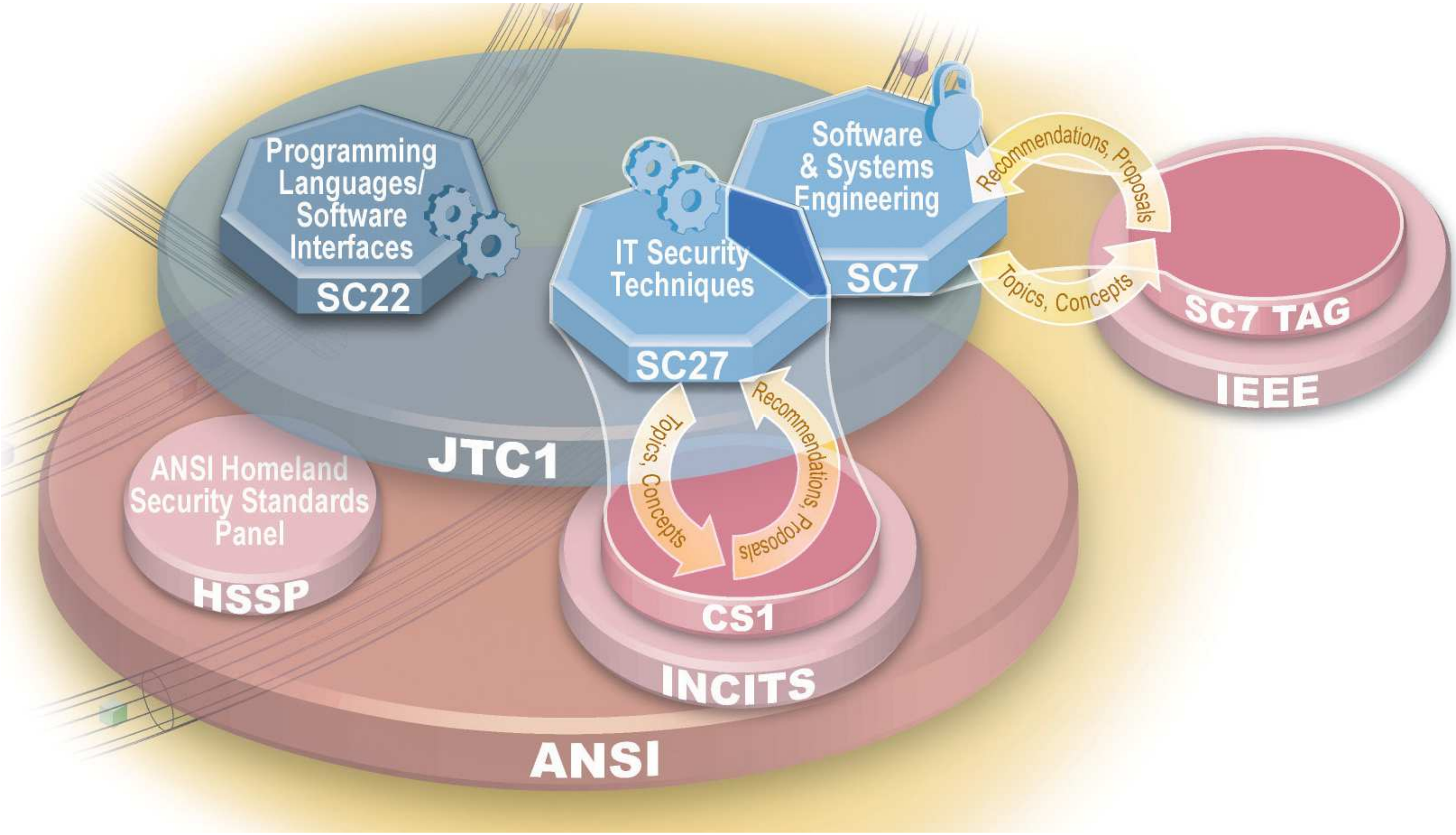
ANSI: HSSP ANSI Homeland Security Standards Panel; INCITS: CS1

Stakeholders: Int'l Govt's; Nat'l Standards Bodies; Companies; Academia; Individuals; Non-Governmental Organizations: Safecode, NDIA

DRAFT

1/12/10

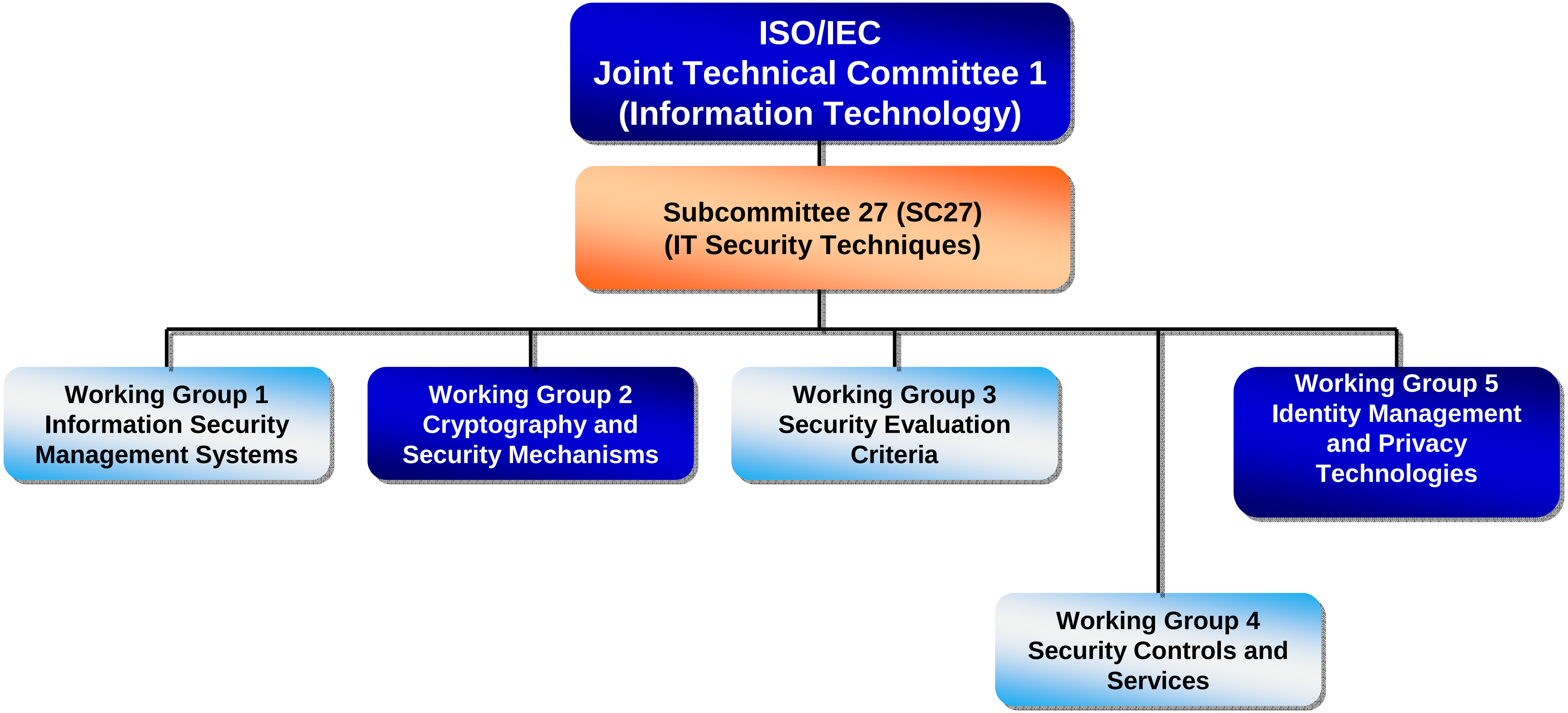
ISO/IEC JTC1 SC7 and ISO/IEC JTC1 SC27 have a substantial number of relevant standards


Programming Languages/ Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
JTC1
Topics, Concepts
Recommendations, Proposals
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI

CS1 ICT SCRM Ad Hoc Group

- Established in February 2009
- Joint with SC7 TAG
- Substantial industry and government participation
- Contributed to several new and under revision standards
- Developed consensus-based USNB proposal for ICT Supply Chain Assurance Standard

ISO/IEC JTC1 SC27 focuses on IT Security Techniques



ISO/IEC
Joint Technical Committee 1
(Information Technology)

Subcommittee 27 (SC27)
(IT Security Techniques)

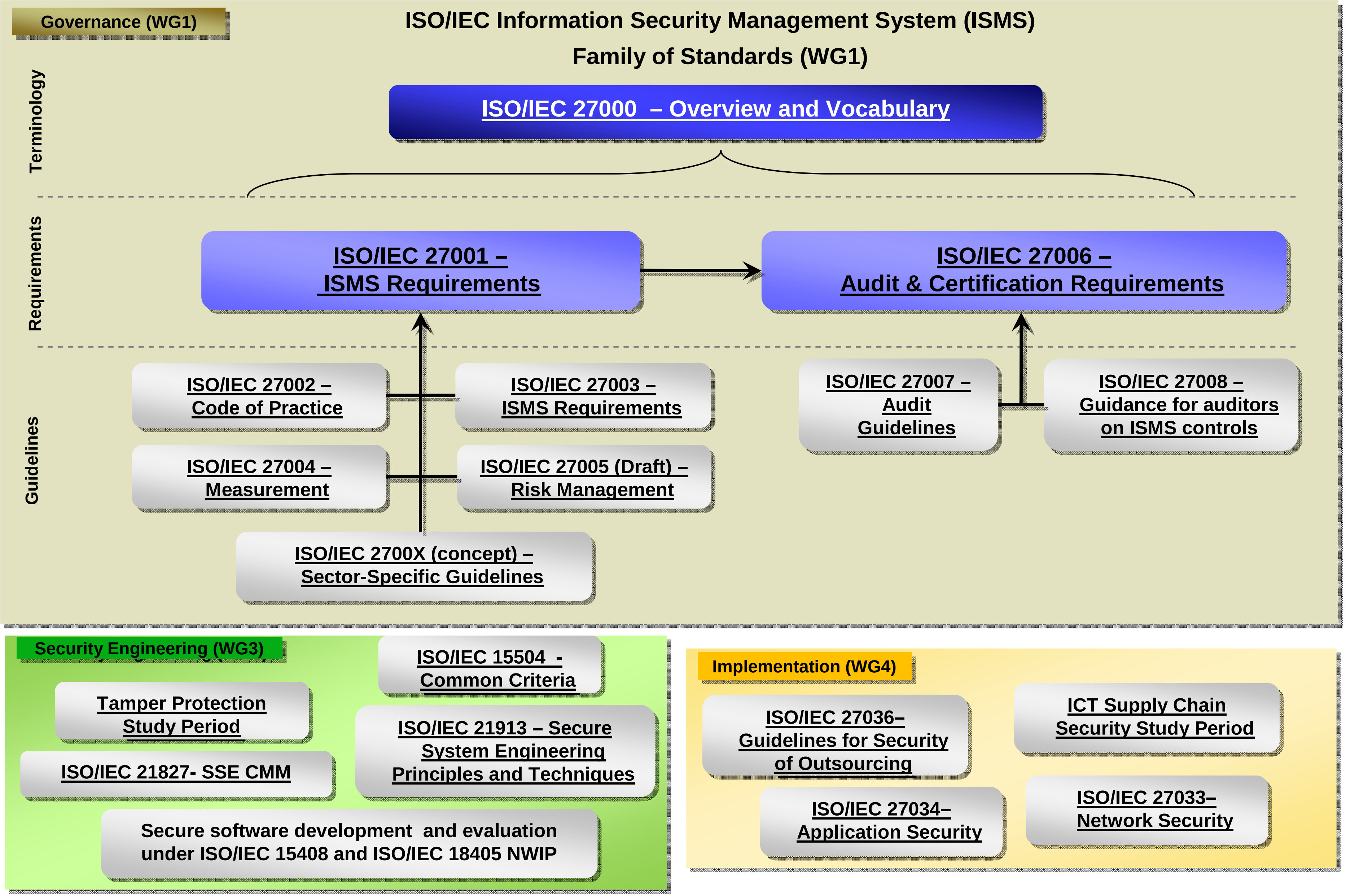
Working Group 1
Information Security
Management Systems

Working Group 2
Cryptography and
Security Mechanisms

Working Group 3
Security Evaluation
Criteria

Working Group 4
Security Controls and
Services

Working Group 5
Identity Management
and Privacy
Technologies



Governance (WG1)

ISO/IEC Information Security Management System (ISMS) Family of Standards (WG1)

Terminology

ISO/IEC 27000 – Overview and Vocabulary

Requirements

ISO/IEC 27001 – ISMS Requirements

ISO/IEC 27006 – Audit & Certification Requirements

Guidelines

ISO/IEC 27002 – Code of Practice

ISO/IEC 27003 – ISMS Requirements

ISO/IEC 27004 – Measurement

ISO/IEC 27005 (Draft) – Risk Management

ISO/IEC 2700X (concept) – Sector-Specific Guidelines

ISO/IEC 27007 – Audit Guidelines

ISO/IEC 27008 – Guidance for auditors on ISMS controls

Security Engineering (WG3)

ISO/IEC 15504 - Common Criteria

Tamper Protection Study Period

ISO/IEC 21913 – Secure System Engineering Principles and Techniques

ISO/IEC 21827- SSE CMM

Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405 NWIP

Implementation (WG4)

ISO/IEC 27036– Guidelines for Security of Outsourcing

ICT Supply Chain Security Study Period

ISO/IEC 27034– Application Security

ISO/IEC 27033– Network Security

ISO/IEC JTC1 WG3 – Security Evaluation Criteria

- Deferred to Bob Martin’s Section of this talk…

ISO/IEC 27034 – Guidelines for Application Security

- **Scope**: The scope of this standard is to specify an application security life cycle, incorporating the security activities and controls for use as part of an application life cycle, covering applications developed through internal development, external acquisition, outsourcing/offshoring1, or a hybrid of these approaches.

- **Purpose and justification**:
  - The standard provides guidance to business and IT managers, developers, auditors, and end-users to ensure that the desired level of security is attained in business applications in line with the requirements of the organization’s Information Security Management Systems (ISMS).
  - Application security addresses all aspects of security required to determine the information security requirements, and ensure adequate protection of information accessed by an application as well as to prevent unauthorized use of the application and unauthorized actions of an application.
  - Informational security concerns in business applications are to be addressed in all phases of the application life cycle, as guided by the organization’s risk management principles and the ISMS adopted.
  - This standard will provide guidance to establishing security goals and includes controls to verify that security target level has been reached. Application Security without any validated controls is a security illusion, and may be more hazardous for the organization.

ISO/IEC 27036 – Guidelines for Security of Outsourcing

- **Scope**: to define guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services. This standard will support the implementation of ISO/IEC 27001/27002 controls for outsourcing and should include the following areas:
  - Strategic goals, objectives and business needs
  - Risks and mitigation techniques
  - Assurance provision

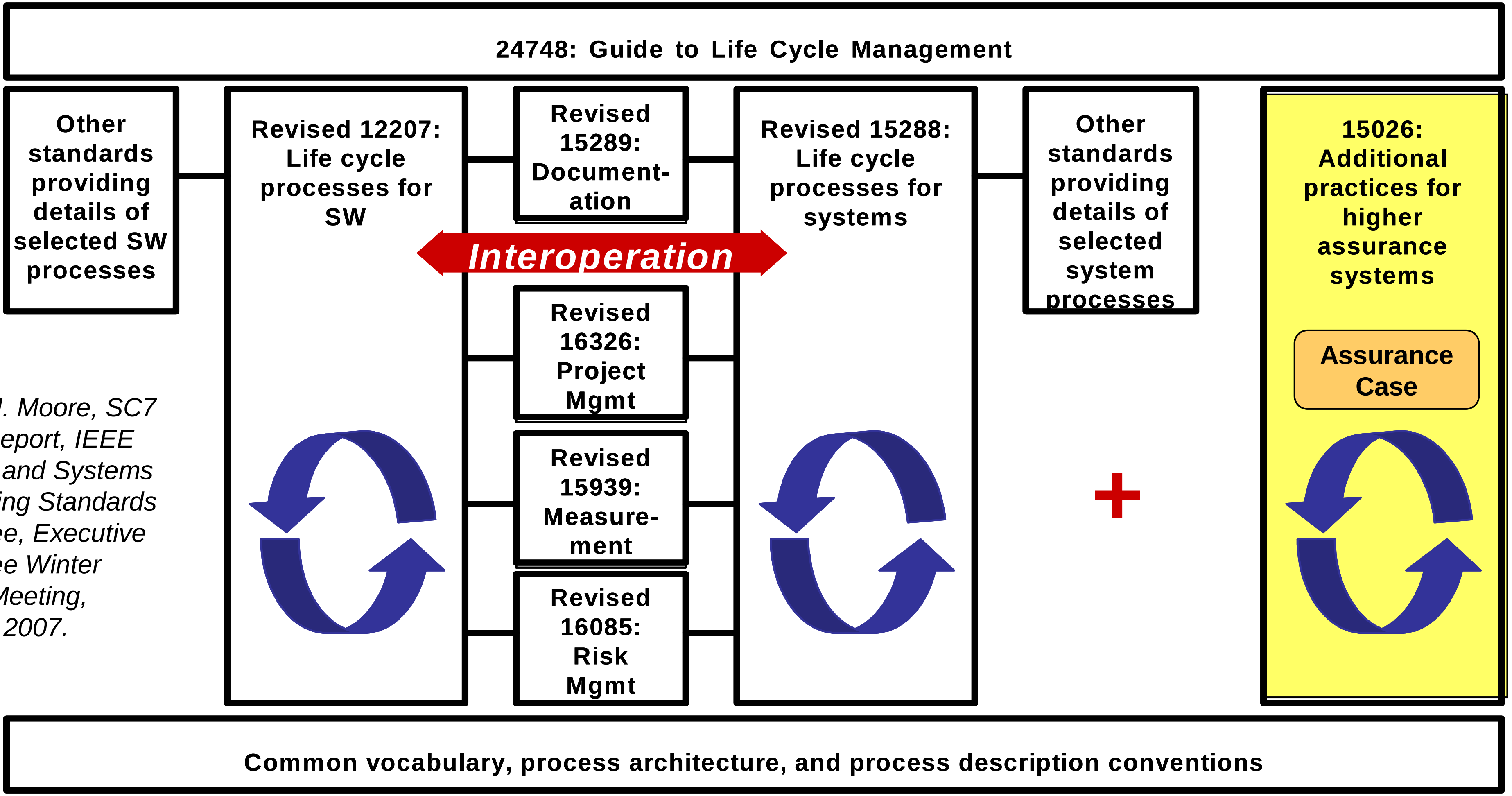
  Note: It is the intent of this standard that outsourcing is not limited to ICT outsourcing, but could include other forms of outsourcing (e.g. human resources, facilities management) that have information security implications.

- **Purpose and Justification**
  - Increased use of IT and back-office operation services outsourcing as one of the means to improve operation efficiency and reduce the total cost of IT and business operations
  - Creation of an extended trust environment that the business units are increasingly depended upon to meet their goals.
  - A number of regulators, in which new security requirements for compliance have been stipulated (Bank of Thailand, 2003; Matsushima, 2000; Yakcop, 2000).
  - Need to provide detailed guidance on applying ISO/IEC 27002 controls relating to outsourcing service providers, in Sections 6.2 (External Parties), and Section 10.2 (Third party service delivery management), including those situations when multiple outsourcing services providers are involved, and when organizations need to change the providers during or at the end of a contractual period.
  - Need to document global commercial sourcing best practices in terms of security from those organizations that have also been managing the security and risk of outsourcing services effectively across different industries.

ICT Supply Chain Security Study Period

- Study Period was proposed by the US, with a draft New Work Item Proposal presented at the WG4 meeting
- WG4 approved a Study Period to address ICT SCRM with a title ICT Supply Chain Security (term Risk Management was challenging)
- Nadya Bartol was appointed a Rapporteur for the Study Period and is responsible for consolidating National Body comments and producing a report with a recommendation to be presented at the May 2010 meeting
- Anticipated result of the Study Period is a New Work Item Proposal to develop a new standard to address ICT SCRM or ICT Supply Chain Assurance
- US submitted a substantial contribution. In addition to DoD, NIST, Microsoft, Boeing, and SAFECode are interested in this work

ISO/IEC JTC1 SC7, System and Software Engineering – Relationship of Key Life Cycle Process Standards



24748: Guide to Life Cycle Management

Other standards providing details of selected SW processes

Revised 12207: Life cycle processes for SW

Revised 15289: Document-ation

Interoperation

Revised 16326: Project Mgmt

Revised 15939: Measure-ment

Revised 16085: Risk Mgmt

Revised 15288: Life cycle processes for systems

Other standards providing details of selected system processes

+

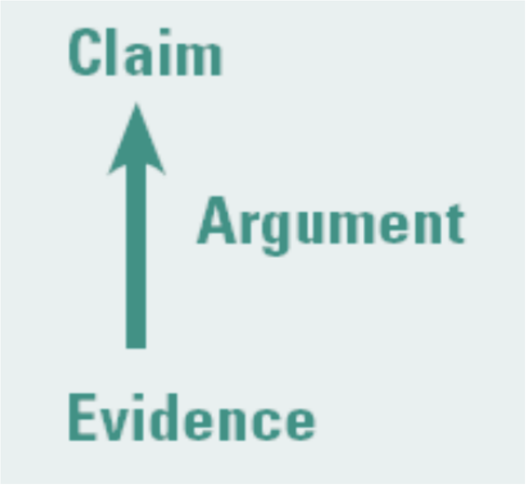
15026: Additional practices for higher assurance systems

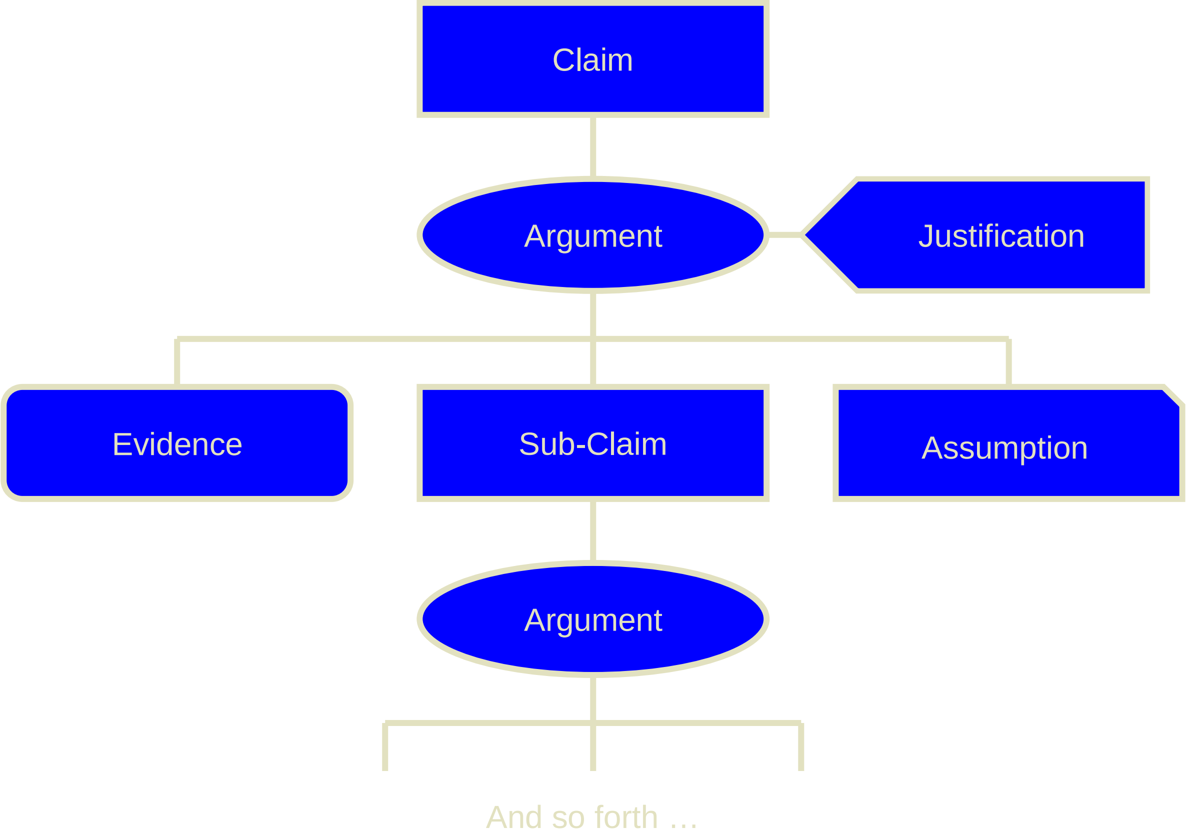
Assurance Case

Common vocabulary, process architecture, and process description conventions

Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

The Assurance Case in ISO/IEC 15026-2





Assurance cases are not new. They are well-grounded in existing practice but with different names and different structures. We are trying to develop a single nomenclature and structure so that safety engineers can talk to security engineers who can talk to reliability engineers, and so forth.

Courtesy of Jim Moore, MITRE

SC22 – Programming Languages

- While we build higher, stronger walls against intrusion…
- … we should also build software that is inherently less vulnerable
- The problem is that some programming languages implicitly encourage coding practices that inherently introduce vulnerabilities
- So, let’s improve the programming languages, or, at least, improve the usage of them in coding

Courtesy of Jim Moore, MITRE

ISO/IEC TR 24772, Programming Language Vulnerabilities

- A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities
- Cross-referenced to CWE
- Each discussion includes
  - Description of the mechanism of failure
  - Recommendations for programmers: How to avoid or mitigate the problem.
  - Recommendations for standardizers: How to improve programming language specifications.
- First edition will be published in 2010
- Second edition will add annexes specific to particular programming languages

Courtesy of Jim Moore, MITRE

Associated Efforts in IEEE Computer Society

- IEEE Computer Society software and systems engineering standards are being “harmonized” with those of ISO/IEC JTC 1/SC 7
  - In some cases, the standards are jointly developed or cross-adopted
  - In other cases, IEEE will offer additional guidance or usage advice.
- Guide to the Software Engineering Body of Knowledge: 2010 Revision
  - In all Knowledge Areas, additional information about basic security practices that are applicable to all software projects.
  - A supplementary Knowledge Area addressing specific practices when security is a specific concern.
- Certified Software Development Professional: 2010 Revision
  - New questions addressing software security
- Consolidate Reference Study (a study syllabus of 13,000 pages of material that software engineers should master)
  - New references addressing software security

Courtesy of Jim Moore, MITRE

What’s next?

- ICT Supply Chain Security Study Period
  - National body contributions are due April 5, 2010
  - Discuss contributions at SC27 April meeting, achieve consensus on way forward, and produce report
  - Results and likely NWIP to be presented in October 2010
- Other inputs – continue working
- Encouraging developments – joint meeting for SC27 WG3/WG4 and SC7 WG7 experts in May 2010
- We need help creating content – please join us at the BoF sessions at this Forum and to the SwA WGs
- Stay tuned…